What is claimed is:

1. A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

identifying a portion of the format information to be encoded;

generating encoded format information from the identified portion of the format information; and

generating encoded digital information, including the digital sample and the encoded format information.

2. The method of claim 1, further comprising the step of requiring a predetermined key to decode the encoded format information.

3. The method of claim 2, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded format information is decoded with the predetermined key.

4. The method of claim 3, wherein the information output from the digital player represents a still image, audio or video.

5. The method of claim 3, wherein the information output represents text data to be authenticated.

6. A method for protecting a digital signal, the digital signal including digital samples in a file format having an inherent granularity, comprising the step of:

creating a predetermined key comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples.

7. The method of claim 6, wherein the digital signal represents a continuous analog waveform.

8. The method of claim 6, wherein the predetermined key comprises a plurality of mask sets.

9. The method of claim 6, wherein the digital signal is a message to be authenticated.

10. The method of claim 6, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

11. The method of claim 6, further comprising the step of:

using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

12. The method of claim 6, wherein the digital signal represents a still image, audio or video.

13. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

validating the mask set at the start of the transfer function-based mask set.

14. The method of claim 13, wherein said step of validating comprises the step of:

comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

15. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

authenticating the mask set by comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

16. The method of claim 13, wherein said step of validating comprises the step of:

comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

17. The method of claim 6, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

authenticating the mask set by comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

18. The method of claim 13, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

19. The method of claim 6, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital signal, wherein the hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying the transfer function-based mask set.

20. A method for protecting a digital signal, the digital signal including digital samples in a file format having an inherent granularity, comprising the steps of:

creating a predetermined key comprised of a transfer function-based mask set that can manipulate data at the inherent granularity of the file format of the underlying digitized samples;

authenticating the predetermined key containing the correct transfer function-based mask set during playback of the data; and

metering the playback of the data to monitor content.

21. The method of claim 20, wherein the predetermined key is authenticated to authenticate message information

22. A method to prepare for the scrambling of a sample stream of data, comprising the steps of:

generating a plurality of mask sets to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;

obtaining a transfer function to be implemented;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

23. A method to prepare for the encoding of stega-cipher information into a sample stream of data, comprising the steps of:

generating a mask set to be used for encoding, the set including a random primary mask, a random convolution mask, and a random start of message delimiter;

obtaining a message to be encoded;

compressing and encrypting the message if desired;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting the message size equal to the total number of bits in the message bit stream.

24. The method of claim 23 wherein the sample stream of data has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

25. The method of claim 13, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

processing the initial series of random bits through an MD5 algorithm;

using the results of the MD5 processing to seed a triple-DES encryption loop;

cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and

concatenating the triple-DES output bits into the random series of bits.

26. A method for copy protection of digital information, the digital information including a digital sample and format information, comprising the steps of:

identifying a portion of the digital sample to be encoded;

generating an encoded digital sample from the identified portion of the digital sample; and

generating encoded digital information, including the encoded digital sample and the format information.

27. The method of claim 26, further comprising the step of requiring a predetermined key to decode the encoded digital sample.

28. The method of claim 27, wherein the digital sample and format information are configured to be used with a digital player, and wherein information output from the digital player will have a degraded quality unless the encoded digital sample is decoded with the predetermined key.

29. The method of claim 27, wherein information output will have non authentic message data unless the encode digital sample is decoded with the predetermined key.